SUBSTITUTION-BASED APPROACH FOR LINGUISTIC STEGANOGRAPHY USING ANTONYM

FAWWAZ ZAMIR BIN MANSOR

A thesis submitted in
fulfillment of the requirement for the award of the
Degree of Master of Information Technology

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

DECEMBER 2017

For my father and mother.

ACKNOWLEDGEMENT

In the name of Allah, The Beneficent, The Merciful, none of this would have been possible. First, I am grateful to ALLAH S.W.T for his blessings and for giving me enough courage to complete my Master in Information Technology. Secondly, I would like to thank my family for their morale support and encouragement in completing my projects and also throughout my study at UTHM as they are my inspiration to success. Not forgetting, I want to pay special gratitude to my supervisor Prof. Madya Dr. Aida Binti Mustapha for guiding and supervising my master project throughout these few semesters. She has been very helpful to me in finishing my project and I appreciate every advice that she has given me by correcting my mistakes. Credit also goes to all my lecturers and everyone who have shared with me their knowledge, cooperation and guidance that is related to my project. Finally, I want to thank all my friends who have given me valuable advice and encouragement in completing my project. Thank you very much to all and May ALLAH bless you all.

ABSTRACT

Steganography has been a part of information technology security since a long time ago. The study of steganography is getting attention from researchers because it helps to strengthen the security in protecting content message during this era of Information Technology. In this study, the use of substitution-based approach for linguistic steganography using antonym is proposed where it is expected to be an alternative to the existing substitution approach that using synonym. This approach still hides the message as existing approach but its will change the semantic of the stego text from cover text. A tool has been developed to test the proposed approach and it has been verified and validated. This proposed approach has been verified based on its character length stego text towards the cover text, bit size types of the secret text towards the stego text and bit size types of the cover text towards the stego text. It has also been validated using four parameters, which are precision, recall, f-measure, and accuracy. All the results showed that the proposed approach was very effective and comparable to the existing synonym-based substitution approach.

ABSTRAK

Steganografi merupakan salah satu cabang daripada keselamatan teknologi maklumat sejak dahulu lagi. Kajian mengenai steganografi semakin mendapat perhatian daripada pengkaji erana ianya membantu memperkasakan keselamatan khususnya dalam melindungi kandungan mesej dalam era teknologi maklumat ini. Dalam kajian ini, penggunaan linguistik steganografi menggunakan kaedah penggantian antonim diusulkan di mana ianya dijangkakan akan menjadi alternatif kepada kaedah sedia ada yang menggunakan sinonim. Kaedah ini masih menyembunyikan mesej seperti kaedah sedia ada tetapi ianya akan mengubah semantik dalam teks stego daripada teks medium. Sebuah alat telah dibangunkan untuk menguji kaedah yang dicadangkan dan ianya telah diuji melalui proses verifikasi dan validasi. Kaedah ini diverifikasi berdasarkan panjang aksara teks stego kepada teks medium, jenis saiz bit teks rahsia kepada teks stego, dan juga jenis saiz bit teks medium kepada teks stego. Ianya juga divalidasikan menggunakan empat parameter iaitu kejituan, ingatan, ukuran-f dan ketepatan. Semua keputusan menunjukkan bahawa kaedah yang dicadangkan adalah sangat efektif dan setara dengan penggantian sinonim sedia ada.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF PUBLICATIONS

Fawwaz Zamir Mansor, Aida Mustapha, Noor Azah Samsudin. (2017). Researcher's Perspective of Linguistic Steganography on Substitution Method. In *Proceedings of the International Conference on Advances in Computing and Intelligent System* (ICACIS 2017), 6 May 2017, Melaka, Malaysia.

Hanizan Shaker Hussain, Roshidi Din, Aida Mustapha, Fawwaz Zamir Mansor. 2017. LSB Algorithm based on Support Vector Machine in Digital Image Steganography. *Journal of Telecommunication Electronic and Computer Engineering*, 9(2-12):7-12.

Nazim Razali, Fawwaz Zamir Mansor, Syahdan Mahad Hamzah. (2017). Pattern Analysis of Goals Scored for Association Football. Silver Award. *Data Analytic Industry Challenge in 2017 CREST Industry Data Analytical Challenge* (Southern Region).

CHAPTER 1

INTRODUCTION

1.1 Research Background

Text document is one of the important medium of information until the present times even though a lot of other mediums had been established (Sheldon, 2017). The need for text documents is still high in the domain of business and academic. It is because a lot of important documented information such as appointment letter, certification, report, confidential document and other documents are presently available in text. Therefore, text documents should be a concern for everyone because information and communication have a lot of risk. The intruders occasionally temper with information and communication for their own interests. The text document, which is commonly confidential information, becomes their target to discover the secret information that could be used for illegal purposes. Hence, a special technique named steganography is introduced to overcome this problem.

Steganography is best known as an associated knowledge of hiding the messages via mediums of data to become invisible and undetectable from the human sense. Securing private information is a critical point of steganography in applying performance as a part of information hiding. The practice of idea steganography has been used since the ancient times (Iyer & Lakhtaria, 2016). The implementation of steganography itself is divided into two categories. Firstly; the implementation of steganography in different mediums of image, audio, video and other digitally invisible code namely technical steganography. Secondly; the implementation of steganography in the medium of text is known as text steganography. It is anticipated

that the steganography approach can give some solution for safeguarding the security of information in the text media.

The implementation of text steganography is by hiding the secret text in the medium of text so that the third party is unable to discover the existence of the message. In other words, steganography in the medium of text can make the secret information invisible and unnoticed for third party to see or detect, and it is directed to the appropriate receivers to apprehend the information. However, steganography in the text domain is the most challenging method of operation compared to the other domains. The challenge in implementing steganography in the text domain since the text file has a small quantity to hide information (Nasab & Shafiei, 2011) and it depends on the limited space available in the text. Nevertheless, this study is specifically focused in the steganography method in the text domain.

There are two groups of text steganography. The first is linguistic steganography. This type of steganography is dependable on the linguistic order of the sentence of text. The second is the format-based steganography which manipulates the component of text such as word, line, space and other components of text to hide the message. Specifically, this study focuses on linguistic steganography categories to evaluate the development of this method called substitution method. This method is able to hide the secret texts by embedding them in the text based on the replacement of another text in the original text. This study has chosen some techniques in the substitution-based as the medium to design the model. Then, the design of the model evaluates through some of the parameters that have been chosen for this study.

1.2 Problem Statements

The general issue that acts as driving force for this research is all of proposed techniques for steganography still have to be improvised in number of ways. The existing implementation of the substitution-based approach in linguistic steganography is using the synonyms. One particular evidence is the synonym paraphrasing technique in Spanish language that is very easy to attack (Muñoz, Carracedo, & Álvarez, 2010). In addressing the problem where the stego message still has the same meaning as the cover text, this study proposes for the use of

antonym-based substitution, in an effort to mask the meaning of the cover text. Most of the existing study of substitution-based linguistic steganography apply the synonym-based approach. Therefore, there is a need to study the antonym-based approach as an alternative to implement linguistic steganography. Lastly, the effectiveness of this study will be evaluated using verification and validation techniques.

1.3 Research Question

Based on the problem formulation, the following research questions have been generated;

(i) How to formalise a substitution-based approach using the antonym of words?
(ii) How to develop the antonym-based substitution approach in the linguistic steganography domain?
(iii) How to evaluate the performance of the proposed antonym-based substitution approach in the linguistic steganography domain?

1.4 Objectives of Study

The main goal of this research is to propose a new substitution-based algorithm based on antonyms. In order to achieve this goal, the following objectives must be fulfilled:

(i) To formalise an antonym-based substitution approach for linguistic steganography.
(ii) To develop the antonym-based substitution approach on the text domain.
(iii) To evaluate the performance of the proposed antonym-based substitution approach on the text domain.

1.5 Scope of Study

This study focuses on the implementation and measurement of substitution-based techniques of the steganography model on text domain. It consists of the types of steganography method, types of linguistic steganography technique, and parameter measurement.

1.6 Significance of Study

The proposed antonym substitution-based approach in the linguistic steganography technique is valuable in the field of information hiding, specifically by providing the method criteria and scheme design in developing the approach in terms of model or system. It is also beneficial in figuring out the output of the study by encouraging to improve the development system based on the proposed approach through evaluation metrics.

1.7 Organization of Thesis

This chapter presents the basis of the steganography area by covering secret text in the text domain by explaining the background of study, problem formulation, research questions, research objectives, and research scope of this study. In general, this chapter illustrates the steganography area in terms of its kind of area, categories, domain, until the methods of this research which focuses on the text domain steganography that uses linguistic steganography. Figure 1.1 shows that the proposed research consists of three phases; theoretical study, experimental design, and output environment.

- Theoretical Study
    - In this phase, the text steganography that consists of linguistic steganography are reviewed. Then, measurements in the form of verification and validation are also reviewed to identify the limitation and criteria of method used for improvement. It delivers the summary of literature and documentation of problem formulation.
- Experimental Design

- This phase prepares research data and studies the approach that can be used. This study will design and develop a tool to generate stego message. The proposed approach will be implemented into the tool for dataset testing.

- Output Environment
  - This phase will evaluate the performance of the tool using the parameter of each verification and validation processes. The result of the experiment is analysed from the evaluation process environment based parameter metrics. The measurement justifies the results of the verification and validation processes the stego text from the embedding process to become the output data in this environment. This phase can meet the simplified standard measurement in linguistic steganography based on verification and validation processes.

The phases that are employed from this research are based on requirement of the linguistic steganography technique using substitution-based in text steganography. Then, the following input in the categories that used in steganography on the text domain will be presented in Chapter Two.

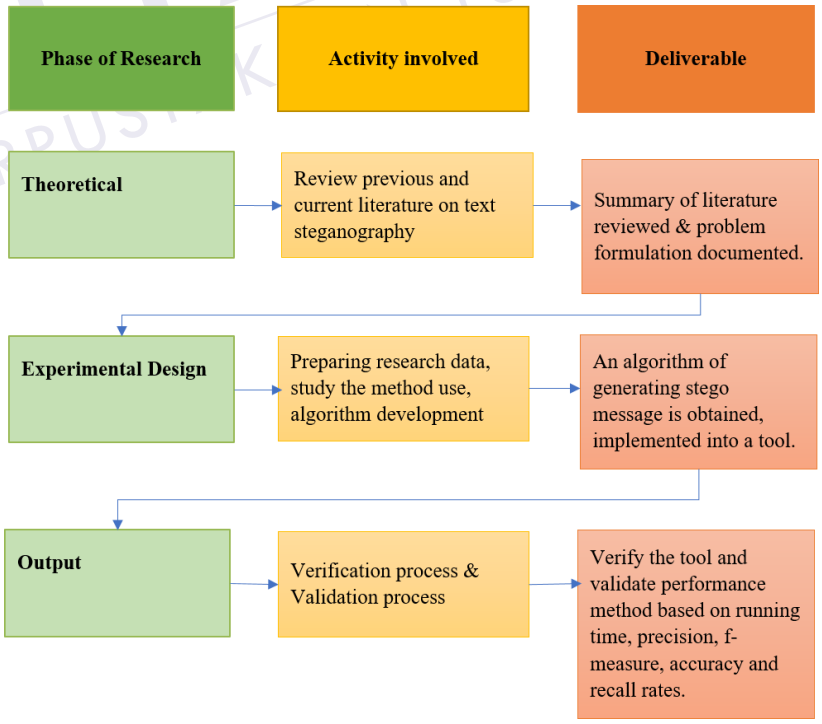

Figure 1.1: The Outline of Phase in the Proposed Research

CHAPTER 2

LITERATURE REVIEW

This chapter contain the literature of text steganography and the relation between each type of text steganography with an elaboration on each of them. Previous approaches on different types of text steganography will also be discussed in this chapter. The advantages and disadvantages of different approaches of linguistic steganography will also be presented together with examples.

2.1 Introduction

Nowadays, the state of privacy level in communication is at risk. The existence of intruders in the communication technology enables anyone to easily retrieve information. The irresponsible intruders or attackers may disclose the secret information to uninvolved parties to check or modify it for abusing that information (Amin et al., 2003). The easy access on the internet increases the chance for attackers and intruders. Therefore, it is our responsibility to take additional measures to ensure the right is well protected. Steganography is the art and science of communicating in such way that the presence of a message cannot be detected. It means covered writing or to hide in plain sight. The main goal of steganography is to hide the fact that a covert communication is present within an innocuous communication (Cox, 2008).

Generally, the process steganography in text domain analogically can be illustrate using Figure 2.1. It illustrates the basic steganography system where the first stage of the production process is to embed the secret message into the pit-selected cover medium and the key to derive the secret message is injected alongside the secret message. The process resulted in a stego medium. If the cover material

used is a text, then the resulting product of the first stage of steganography process is stego text. The same principle is applied with all other steganography cover medium used such as audio, image and video.

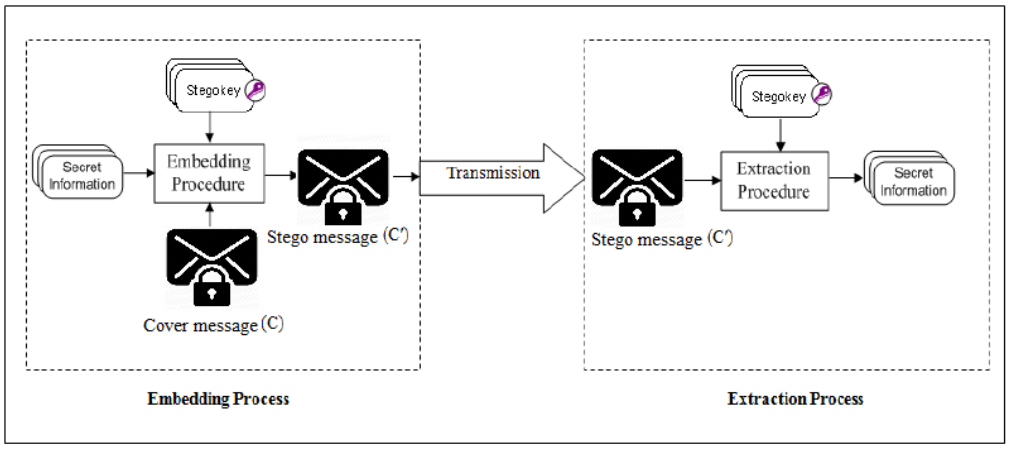

Figure 2.1: Basic Model of Steganography System (Atawneh & Sumari, 2013)

This chapter presents a survey of steganography focusing on the text medium. It also discusses linguistic steganography for comparison, with the objective to signify the classification technique in steganography. This chapter also reviews the categories of linguistic steganography approach that have been used by previous researchers.

2.2 Domain in Text Steganography

Text steganography cover the secret text in the medium of the text. It can be divided into two main categories; format-based steganography and linguistic steganography. Format-based steganography cover the secret text which changes the format in the text such as, word, space, line and any other characters in the sentence of the text. Whereas, linguistic steganography covers the secret text by modifying the information that is encoded based on linguistic order (Chang & Clark, 2010). The classification of text steganography is presented in Figure 2.2.

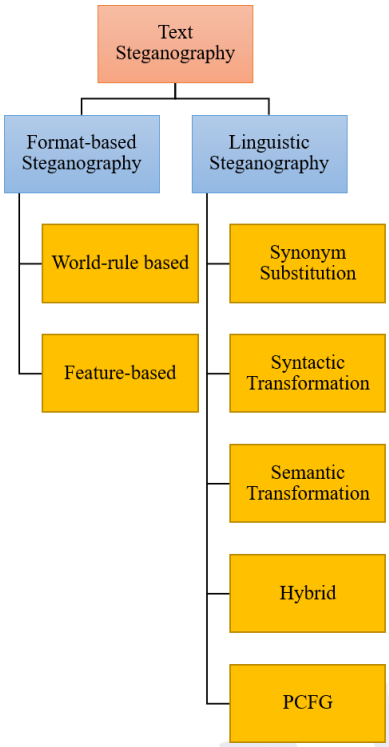

Figure 2.2: Classification of Text Steganography

The techniques of steganography in the text domain based on Figure 2.2 are classified as format-based steganography and also as linguistic steganography. The development of format-based consists of two kinds of techniques, which are word-rule based and feature-based. Word rule-based is the technique that embeds the secret text based on word pattern by shifting in the text. The techniques consist of line-shift coding and word-shift coding. Line-shift coding hides the secret text by vertically shifting the secret text in the text lines. Meanwhile, word-shift coding hides the secret text by horizontally shifting the secret text in length between words (Bharti & Kumar, 2014).

The second format-based steganography is feature-based that can be defined as a technique that alters the unique featured characteristic in the text based on code words. This technique covers the secret text based on the pattern of the letter or length of the word that conceals and it seems no changes have happened in the text (Nasab & Shafiei, 2011).

For linguistic steganography, the development of approach of hiding secret text includes synonym substitution, syntactic transformation, semantic

transformation, probabilistic context-free grammar (PCFG). Synonym substitution constitutes an approach that substitutes the chosen words with the synonym part of text and modifies more on the grammatical sentences and uninvolved operating structure. Words of language that have a lot of synonyms will obtain more options to hide the information in the text (Chang & Clark, 2010). Then, syntactic transformation known as a technique that uses punctuation marks in text like comma (,) stop (.) to hide information in binary bits of 0 and 1 (Bharti & Kumar, 2014). Furthermore, semantic transformation is an approach that uses two or more semantically similar words with different meaning to translate back and forth that converts to binary bits for hiding the secret text in words (Grothoff et al., 2009).

Meanwhile, probabilistic context-free grammar (PCFG) illustrates the technique in linguistic steganography that hides the information from the generative model. It describes the structures hierarchal three-shaped primary sentences in the given interest domain. It also provides the distribution of probability on sentences that are used to provide decision for some task in the text (Corazza & Satta, 2007). The final approach in linguistic steganography is the hybrid technique that combines two or more methods in the process of hiding information in one text.

2.3 Format-based Steganography

This section presents the text steganography formats which are divided into two parts. The first part presents the word-rule base that consists of two techniques, line-shift coding and word-shift coding. The second part presents the feature-based in format-based steganography that contains techniques based on the unique characteristics that are language based and letter-based.

2.3.1 Word Rule-based

The implementation of word rule-based technique is divided into two kinds of technique to hide the message. The first technique, line-shift coding can embed vertically the secret texts to conceal the message in the text. Meanwhile, the second technique, word-shift coding can embed horizontally the secret text to conceal the message in the text.

2.3.2 Feature-based

The feature-based method modifies the feature of the letter by manipulating the shape, size, and position of the font in the text. The feature-based technique makes it hard for the reader to identify the secret text in the text. The technique of feature-based makes the reader unable to identify the secret information in the text (Roy & Manasmita, 2011). Then, because of the characteristics of this technique, the feature-based could be used by many researchers based on the characters of the language of the world.

2.4 Linguistic Steganography

Linguistic steganography covers the secret information concerned with the language of word and order modification linguistically for encoding the message. This section presents the linguistic steganography that used the steganography technique. Most of the techniques in linguistic steganography had been used in the synonym substitution-based. Synonym substitution-based can be used in any language as long as the language in the text of language has a synonym word. The scholarly papers that have researched linguistic steganography in the last decade are presented in Table 2.1.

Table 2.1: Scholar Paper on Linguistic Steganography

Scholar Author	Specific Methods	Advantage	Disadvantage
(Yuling, Xingming, Can, & Hong, 2007)	Chinese text	Simple and effective variants	Limited capacity on type of word uses
(M. H. Shirali-Shahreza & Shirali-Shahreza, 2008)	English text (UK and US)	Suggested to use in printing the text electronically	Uses of English word simply easy to attack because of minor differentiation
(Lu, JianBin, TianZhi, & DingYi, 2009)	Chinese text using Word Sense Disambiguation (WSD)	Improved the anti-attack watermarking ability and high robustness.	Reliable with WSD tools.

Table 2.1 (Continued): Scholar Paper on Linguistic Steganography

Scholar Author	Specific Methods	Advantage	Disadvantage
(Muhammad, Shakil, & Syed Ahmad Abdul Rahman, 2009)	Malay linguistic	High invisibility	Requires much time on the complexity of word access
(Muñoz et al., 2010)	Spanish language using synonym paraphrasing	Obvious capable use in Spanish language	Easy to attack and slight volume number
(Chang & Clark, 2010)	English text using SemEval lexical	High possibility of using a suitable word for replacement.	High preservation of the grammar text
(Cao Qi, Sun Xingming, & Xiang Lingyun, 2013)	Traditional synonym substitution	Large volume and recommended to avoid steganalysis	Complex algorithm that requiring big dataset
(Wang, Huang, Chen, Yang, & Miao, 2013)	English text using context-based	Minimise to create the syntax error that suggests the concealment steganography.	Lack of vocabulary and narrow scales dictionaries

From Table 2.1, the text steganography identified the advantages and disadvantages of linguistic steganography during the last decade. The advantages of techniques based on Table 2.1 are highlighted as follows;

- Unlike the feature-based steganography approach, linguistic steganography especially in the synonym substitution-based technique that has its own implementation performance; high invisibility in Malay linguistic techniques(Muhammad et al., 2009) and English text using LUNABEL function (Chand & Orgun, 2006), a simple variant in Chinese text synonym (Yuling et al., 2007), and minimised to create syntax error in English text using context-base maximum cumulative distortion (Topkara, Topkara, & Atallah, 2006).
- The traditional synonym substitution technique (Qi et al., 2013) can also hide secret texts in large capacity.
- Linguistic steganography has an advantage in specific conditions and are useful in printing text using synonym substitution (Shahreza, 2008). Other

techniques have this advantage of synonym paraphrasing which is very useful in Spanish language (Muñoz et al., 2010).

- Some approaches in feature-based has privilege protection embedded in the secret text like high robustness in a rectangular region technique in Chinese based (Wenyin Zhang, Zhenbin Zeng, Geguang Pu, & Huibiao Zhu, n.d.), numerical code technique in Hindi based (Pathak, 2010) and one of the approaches recommended in feature-based is able to change alphabet letter pattern approach to avoid steganalysis (Bhattacharyya et al., 2011).

Meanwhile, this research also identified the disadvantages in this technique based on Table 2.1 which are;

- Low security is also the issue in linguistic steganography approach especially in synonym substitution-based (Shahreza, 2008) and the technique of synonym paraphrasing in Spanish language is easy to attack (Muñoz et al., 2010).
- The obvious issue in implementing linguistic steganography is only useful in its own language because this technique is based on linguistic and other limitation of this technique as it has a complex algorithm in the English text using LUNABEI function (Chand & Orgun, 2006) and traditional synonym substitution (Cao Qi et al., 2013). In an English text using context-based it has incomplete vocabulary (Wang et al., 2013). Then, in the semantic transformation of the technique the performance possibly generates a lot of semantic spam.
- The time consumption in the process of embedding/extracting secret text in the text was also a disadvantage in the linguistic steganography technique like Malay linguistic (Muhammad et al., 2009).

2.5 Substitution-based

Distinguishable from other methods that were described before, the substitution method is not only able to maintain the syntax of a sentence but also its original

meaning as a whole. It employs existing words or paragraphs as cover text and replaces the words with any appropriate counterpart. The advantages of this technique lay in its flexibility of source point like newspapers, websites, magazines, novels etc.

At present, only one type of substitution-based approach exists in the literature, which is synonym-based substitution by Winstein (1998). He utilised WordNet (1995) as a database for words that are readily classified according to their synonym as a substitution set in his method. His early approach, the naive algorithm, only replaces words in their original contexts without considering the meaning. The WordNet-dependent substitution set does not aid in accurately extracting the meaning of each word. This is due to the fact that WordNet will only list down the synonym for each given word. As example, the word "too" that is fed to the WordNet will produce the following results:

1. (excessively, overly, too)
2. (besides, too, also, likewise, as well)

The meaning of resulting synonyms has different usage properties as they are counted as a substitution set by Winstein's algorithm. It is not possible for the word "too" in the sentence "this car is too expensive compared to the other car" to be replaced with the word "also". This shows that "too" and "also" cannot be simply interchanged even though both sit in the same set of synonyms. In response, Winstein added a few rules to the WordNet synonym set. By doing so, 30% of the WordNet words were merged into several interchange sets. Even though it managed to reduce substitution of the same word, it still lacks the accuracy of the word's meaning in certain context.

Several studies on synonym substitution have been completed to enhance the core segment of earlier studies and maintain a correct and cohesive semantic aspects of the text (Bolshakov, 2004;Shahreza, 2008). The primary objective of the synonym substitution method is to enable the system to automatically opt for the synonym selected from possible candidates who possesses syntactically and semantically correct text who is as good as human choice (Chapman, 2001).

In citing the works done who applied the concept of synonym on the simple message system (SMS) and changing the word spelling in British-America terms

REFERENCES

Alam, M. N., & Naser, M. A. (2014). Re-evaluating chain-code as features for Bangla script. In *2013 International Conference on Electrical Information and Communication Technology (EICT)* (pp. 1–5). IEEE. https://doi.org/10.1109/EICT.2014.6777865

Alves, G. I. L., Silva, D. A., Pereira, E. J. S., & Ferreira, T. A. E. (2013). Data Envelopment Analysis for Selection of the Fitness Function in Evolutionary Algorithms Applied to Time Series Forecasting Problem. In *2013 BRICS Congress on Computational Intelligence and 11th Brazilian Congress on Computational Intelligence* (pp. 534–539). IEEE. https://doi.org/10.1109/BRICS-CCI-CBIC.2013.94

Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003). Information hiding using steganography. In *4th National Conference on Telecommunication Technology, NCTT 2003 - Proceedings* (pp. 21–25). IEEE. https://doi.org/10.1109/NCTT.2003.1188294

Atawneh, S., & Sumari, P. (2013). Hybrid and Blind Steganographic Method for Digital Images Based on DWT and Chaotic Map. *Journal of Communications*, *8*(11), 690–699. https://doi.org/10.12720/jcm.8.11.690-699

Bharti, D., & Kumar, A. (2014). Enhanced Steganography Algorithm to Improve Security by using Vigenere Encryption and First Component Alteration Technique. *International Journal of Engineering Trends and Technology (IJETT)*, *13*(5), 242–246. https://doi.org/10.14445/22315381/IJETT-V13P250

Bhattacharyya, S., Indu, P., Dutta, S., Biswas, A., & Sanyal, G. (2011). Hiding Data in Text Through Changing in Alphabet Letter Patterns (CALP). *Journal of Global Research in Computer Science*, *2*(3), 33–39.

Bhattacharyya, S., Kshitij, a. P., & Sanyal, G. (2010). A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform. In *Recent Trends in Information, Telecommunication and Computing (ITC),*

2010 International Conference on (pp. 173–178). IEEE. https://doi.org/10.1109/ITC.2010.68

Bolshakov, I. A. (2004). A Method of Linguistic Steganography Based on Collocationally-Verified Synonymy. *Information Hiding: 6th International Workshop*, *3200*(Cic), 180–191. https://doi.org/10.1007/b104759

Buffoni-Rogovchenko, L., Fritzson, P., Nyberg, M., Garro, A., & Tundis, A. (2013). Requirement Verification and Dependency Tracing During Simulation in Modelica. In *2013 8th EUROSIM Congress on Modelling and Simulation* (pp. 561–566). IEEE. https://doi.org/10.1109/EUROSIM.2013.99

Cao Qi, Sun Xingming, & Xiang Lingyun. (2013). A secure text steganography based on synonym substitution. In *IEEE Conference Anthology* (pp. 1–3). IEEE. https://doi.org/10.1109/ANTHOLOGY.2013.6784896

Chand, V., & Orgun, C. O. (2006). Exploiting Linguistic Features in Lexical Steganography: Design and Proof-of-Concept Implementation. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (p. 126b–126b). IEEE. https://doi.org/10.1109/HICSS.2006.175

Chang, C.-Y., & Clark, S. (2010). Practical Linguistic Steganography using Contextual Synonym Substitution and Vertex Colour Coding. *Emnlp*, *40*(2), 403–448. https://doi.org/10.1162/COLI_a_00176

Changder, S., Das, S., & Ghosh, D. (2010). Text steganography through Indian Languages using feature coding method. In *ICCTD 2010 - 2010 2nd International Conference on Computer Technology and Development, Proceedings* (pp. 501–505). https://doi.org/10.1109/ICCTD.2010.5645849

Changder, S., Debnath, N. C., & Ghosh, D. (2009). A new approach to hindi text steganography by shifting matra. In *ARTCom 2009 - International Conference on Advances in Recent Technologies in Communication and Computing* (pp. 199–202). https://doi.org/10.1109/ARTCom.2009.122

Chen, Y.-R., Su, W.-T., Hsiung, P.-A., Lan, Y.-C., Hu, Y.-H., & Chen, S.-J. (2010). Formal modeling and verification for Network-on-chip. In *The 2010 International Conference on Green Circuits and Systems* (pp. 299–304). IEEE. https://doi.org/10.1109/ICGCS.2010.5543050

Coderre, E. L., Chernenok, M., Gordon, B., & Ledoux, K. (2017). Linguistic and Non-Linguistic Semantic Processing in Individuals with Autism Spectrum

Disorders: An ERP Study. *Journal of Autism and Developmental Disorders*, *47*(3), 795–812. https://doi.org/10.1007/s10803-016-2985-0

Corazza, A., & Satta, G. (2007). Probabilistic context-free grammars estimated from infinite distributions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *29*(8), 1379–1393. https://doi.org/10.1109/TPAMI.2007.1065

Cox, I. J. M. L. J. A. J. T. (2008). *Digital Watermarking and Steganography Book*. Morgan Kaufmann Publishers.

Dulera, S., Jinwala, D., & Dasgupta, A. (2011). Experimenting with the Novel Approaches in Text Steganography. *International Journal of Network Security & Its Applications*, *3*(6), 213–225. https://doi.org/10.5121/ijnsa.2011.3616

Ghumman, W. A., & Lassig, J. (2013). Verification Requirements for Secure and Reliable Cloud Computing. In *2013 International Conference on Cloud and Green Computing* (pp. 143–150). IEEE. https://doi.org/10.1109/CGC.2013.29

Grothoff, C., Grothoff, K., Stutsman, R., Alkhutova, L., & Atallah, M. (2009). Translation-based steganography. *Journal of Computer Security*, *17*(3), 269–303. https://doi.org/10.3233/JCS-2009-0320

Gutub, A. A.-A., & Fattani, M. M. (2007). A Novel Arabic Text Steganography Method Using Letter Points and Extensions. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *1*(3), 483–486.

Ighile, M. (2013, April 26). The Poetry of Igue Festival's Song-Text. *Studies in Literature and Language*. https://doi.org/10.3968/n

Iyer, S. S., & Lakhtaria, K. (2016). New robust and secure alphabet pairing Text Steganography Algorithm. *Ijcter.com*, *2*(7), 15–21. Retrieved from http://www.ijcter.com/papers/volume-2/issue-7/new-robust-and-secure-alphabet-pairing-text-steganography-algorithm.pdf

Kataria, S., Kumar, T., Singh, K., & Nehra, M. S. (2013). ECR (encryption with cover text and reordering) based text steganography. In *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)* (pp. 612–616). IEEE. https://doi.org/10.1109/ICIIP.2013.6707666

Kumar, R., Chand, S., & Singh, S. (2014). An Email based high capacity text steganography scheme using combinatorial compression. *Confluence The Next Generation*. Retrieved from http://ieeexplore.ieee.org/abstract/document/6949231/

Kumar, R., Malik, A., Singh, S., & Chand, S. (2016). A high capacity email based text steganography scheme using Huffman compression. In *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 53–56). IEEE. https://doi.org/10.1109/SPIN.2016.7566661

Lu, H., JianBin, L., TianZhi, L., & DingYi, F. (2009). An anti-attack watermarking based on synonym substitution for Chinese text. In *5th International Conference on Information Assurance and Security, IAS 2009* (Vol. 1, pp. 356–359). https://doi.org/10.1109/IAS.2009.66

Mahato, S., Yadav, D., & Khan, D. (2013). A modified approach to text steganography using hypertext markup language. *Advanced Computing and*. Retrieved from http://ieeexplore.ieee.org/abstract/document/6524271/

Marincic, J., Mader, A., & Wieringa, R. (2011). Validation of embedded system verification models. In *2011 Model-Driven Requirements Engineering Workshop* (pp. 48–54). IEEE. https://doi.org/10.1109/MoDRE.2011.6045366

Memon, J. A., Khowaja, K., & Kazi, H. (2008). Evaluation of Steganography for Urdu / Arabic Text . *Pace Pacing And Clinical Electrophysiology*, 232–237.

Muhammad, H. Z., Shakil, A., & Syed Ahmad Abdul Rahman, S. M. (2009). Synonym based malay linguistic text steganography. In *2009 Innovative Technologies in Intelligent Systems and Industrial Applications, CITISIA 2009* (pp. 423–427). https://doi.org/10.1109/CITISIA.2009.5224169

Muñoz, A., Carracedo, J., & Álvarez, I. A. (2010). Measuring the security of linguistic steganography in Spanish based on synonymous paraphrasing with WSD. In *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010* (pp. 965–970). https://doi.org/10.1109/CIT.2010.178

Nagarhalli, T. P., Bakal, J. W., & Jain, N. (2016). A Survey of Hindi Text Steganography. *International Journal of Scientific & Engineering Research*, *7*(3). Retrieved from http://www.ijser.org

Nanhe, A. M., Kunjir, M. P., Sakdeo, S. V, Tech, B., & Sci, C. (2008). " Improved Synonym Approach to Linguistic Steganography " Design and Proof-of-Concept Implementation. Retrieved from http://dsl.cds.iisc.ac.in/~mayuresh/ImprovedSynonymApproachToLinguisticSte

ganography.pdf

Nasab, M. V., & Shafiei, B. M. (2011). Steganography In Programming. *Australian Journal of Basic & Applied Sciences*, *3*(12), 1496–1499. Retrieved from http://ajbasweb.com/old/ajbas/2011/December-2011/1496-1499.pdf

Nazir, S., Motla, Y. H., Abbas, T., Khatoon, A., Jabeen, J., Iqra, M., & Bakhat, K. (2014). A process improvement in requirement verification and validation using ontology. In *Asia-Pacific World Congress on Computer Science and Engineering* (pp. 1–8). IEEE. https://doi.org/10.1109/APWCCSE.2014.7053837

Odeh, A., Elleithy, K., & Faezipour, M. (2013). Text Steganography Using Language Remarks. Retrieved from https://scholarworks.bridgeport.edu/xmlui/bitstream/handle/123456789/1449/Text Steganography Using Language Remarks.pdf?sequence=1

Odeh, A., Elleithy, K., & Faezipour, M. (2014). Steganography in text by using MS word symbols. In *Proceedings of the 2014 Zone 1 Conference of the American Society for Engineering Education* (pp. 1–5). IEEE. https://doi.org/10.1109/ASEEZone1.2014.6820635

Pathak, M. (2010). A new approach for text steganography using Hindi numerical code. *International Journal of Computer Applications*. Retrieved from https://pdfs.semanticscholar.org/2abe/a871899cc8db91d0d0aa0dbc9ac21ac2a424.pdf

Popa, R. (1998). An analysis of steganographic techniques. *The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering*, 65.

Rahmat, R., Kamel, N. S., & Yahya, N. (2009). Subspace-based signature verification technique using reduced-sensor data glove. In *2009 IEEE Symposium on Industrial Electronics & Applications* (pp. 83–88). IEEE. https://doi.org/10.1109/ISIEA.2009.5356475

Roy, S., & Manasmita, M. (2011). A Novel Approach to Format Based Text Steganography. *Communications in Computer and Information Science*, *142 CCIS*(January 2011), 511–516. https://doi.org/10.1007/978-3-642-19542-6_51

Sargent, R. G. (2015). An introductory tutorial on verification and validation of simulation models. In *2015 Winter Simulation Conference (WSC)* (pp. 1729–1740). IEEE. https://doi.org/10.1109/WSC.2015.7408291

Sheldon, P. (2017). Is Medium the Message? Perceptions of and Reactions to Emergency Alert Communications on College Campuses. In *Digital Transformation in Journalism and News Media* (pp. 467–479). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-27786-8_34

Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2008). A new synonym text steganography. In *Proceedings - 2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2008* (pp. 1524–1526). https://doi.org/10.1109/IIH-MSP.2008.6

Shirali-Shahreza, M., & Shirali-Shahreza, M. H. (2007). Text Steganography in SMS. In *2007 International Conference on Convergence Information Technology (ICCIT 2007)* (pp. 2260–2265). IEEE. https://doi.org/10.1109/ICCIT.2007.100

Sun, X., Meng, P., Ye, Y., & Hang, L. (2010). Steganography in Chinese text. In *ICCASM 2010 - 2010 International Conference on Computer Application and System Modeling, Proceedings* (Vol. 8). https://doi.org/10.1109/ICCASM.2010.5620373

Talip, M., Jamal, A., & Wenqiang, G. (2012). A Proposed Steganography Method to Uyghur Script. In *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 125–128). IEEE. https://doi.org/10.1109/CyberC.2012.101

Topkara, U., Topkara, M., & Atallah, M. J. (2006). The hiding virtues of ambiguity. In *Proceeding of the 8th workshop on Multimedia and security - MM&Sec '06* (p. 164). New York, New York, USA: ACM Press. https://doi.org/10.1145/1161366.1161397

Trillas, E. (2017). Antonyms. Negation, and the Fuzzy Case (pp. 25–34). Springer, Cham. https://doi.org/10.1007/978-3-319-56053-3_3

Usener, C. A., Gruttmann, S., Majchrzak, T. A., & Kuchen, H. (2010). Computer-Supported Assessment of Software Verification Proofs. In *2010 International Conference on Educational and Information Technology*. IEEE. https://doi.org/10.1109/ICEIT.2010.5607766

Wang, F., Huang, L., Chen, Z., Yang, W., & Miao, H. (2013). A Novel Text Steganography by Context-Based Equivalent Substitution. Retrieved from http://or.nsfc.gov.cn/handle/00001903-5/414117

Wenyin Zhang, Zhenbin Zeng, Geguang Pu, & Huibiao Zhu. (n.d.). Chinese Text Watermarking Based on Occlusive Components. In *2006 2nd International Conference on Information & Communication Technologies* (Vol. 1, pp. 1850–1854). IEEE. https://doi.org/10.1109/ICTTA.2006.1684670

Winstein, K. (1998). Lexical Steganography Through Adaptive Modulation of the Word Choice Hash. *IBM Systems Journal*, *35*(3), 247–263. Retrieved from http://web.mit.edu/keithw/tlex/lsteg.pdf

Xinhua, L., Weida, W., & Wenjian, L. (2007). An Intelligent Methodology for Business Process Model Verification. In *2007 IEEE International Conference on Control and Automation* (pp. 2381–2385). IEEE. https://doi.org/10.1109/ICCA.2007.4376788

Yuling, L., Xingming, S., Can, G., & Hong, W. (2007). An Efficient Linguistic Steganography for Chinese Text. In *Multimedia and Expo, 2007 IEEE International Conference on* (pp. 2094–2097). https://doi.org/10.1109/ICME.2007.4285095